Department of Homeland Security Daily Open Source Infrastructure Report for 4 December 2008

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- According to the Knoxville News Sentinel, a new report by the U.S. Department of Energy's Inspector General criticized three sites where protective force officers were not trained to use their 40 mm grenade launchers under reduced visibility. (See item **9**)
- WFTV 9 Orlando reports that Social Security numbers for 250,000 people were accidentally posted online by the Florida Agency for Workforce Innovation in October. (See item **29**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *December 2, Reuters* – (National) **AEP studies transmission lines for renewable power.** American Electric Power announced on December 2 that it is studying the possibility of building a multi-state transmission project in the Upper Midwest United States, to help develop wind power generation. AEP wants to hook up existing 765-kilovolt (kV) lines in the Midwest with proposed 765-kV lines that would bring wind power from North Dakota and later from South Dakota, Iowa, and Minnesota. The proposed project is in "conceptual stage" and would be built in stages, if approved and financed. The transmission project "will likely require more than 1,000 miles of new extra-high voltage transmission lines at a cost of between $5 billion and $10 billion," AEP said. The Midwest Independent System Operator, which manages transmission

lines in the region, must approve the project. The new lines would connect 2,000 megawatts of wind power in Hartland Wind Farm project in North Dakota, near the western terminus of the proposed lines, AEP said. "The Dakotas, Minnesota and Iowa have some of the very best wind generation resources in the United States, but the wind potential in this region cannot be developed unless we build a very efficient transmission superhighway to bring this clean, renewable generation to population and electricity load centers," said AEP's chairman, president, and CEO.
Source:
http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSN0227398220081203

2. *December 2, Dow Jones* – (National) **Supreme Court looks for middle ground on power plant regs.** The U.S. Supreme Court Tuesday sought middle ground as it debated whether to overturn a lower court ruling that could make it harder for power plants to avoid expensive updates to aging cooling tower systems. The outcome is important to utility companies with traditional water-cooled generating facilities. Entergy Corp., utility industry groups, and power companies want to revive a 2004 Environmental Protection Agency regulation that allowed the cost of updating cooling tower systems to be weighed against the potential environmental benefits of making the changes. At oral arguments the Supreme Court appeared split. The rules at issue would allow the cost-and-benefit analysis be done before a power plant is forced to change an open-cycle system that withdraws and discharges large amounts of water from streams, lakes, or dam impoundments. This process is common in electricity generation, but both the intake and discharge of water has a larger environmental impact than closed-cycle systems that recycle water repeatedly or dry-cycle systems that rely on air for cooling.
Source:
http://money.cnn.com/news/newsfeeds/articles/djf500/200812021335DOWJONESDJONLINE000548_FORTUNE5.htm

3. *December 2, Associated Press* – (Arkansas) **Work on Ark. power plant halted after appeal filed.** An appeal of the state's decision to grant an air permit for a proposed $1.5 billion coal-fired power plant in southwest Arkansas brought the project to a halt, idling 400 workers. The work stopped on Monday when Southwestern Electric Power Co. (SWEPCO) learned of the appeal, filed by the Sierra Club and Audubon Arkansas with the Arkansas Pollution Control and Ecology Commission. A SWEPCO spokesman said the automatic shutdown was required as part of the permit whenever an appeal is filed. He said the company would ask the commission to allow construction to resume while a decision is pending on the appeal. "The construction of the project is not adversely affecting air quality and we believe it should be allowed," he said. The Arkansas Department of Environmental Quality issued the permit November 5 after reviewing the project for more than two years.
Source:
http://money.cnn.com/news/newsfeeds/articles/apwire/514ef259312a55371ea21afeee33f751.htm

[Return to top]

Chemical Industry Sector

4. *December 2, Frederick News-Post* – (Maryland) **Chemical company calls Frederick allegations untrue.** The head of a company that will no longer supply water treatment chemicals to the City of Frederick said false allegations persuaded elected officials to terminate a contract. The chief executive officer of Sarasota, Florida-based JCI Jones Chemicals Inc. said containers of chlorine and sulfur dioxide are thoroughly checked before they leave the company's plants. The Board of Aldermen unanimously voted to cancel the contract after city workers complained of corroded containers and valves that were nearly impossible to open. The steel containers are directly connected to the water and waste water treatment systems. The 150 pound containers hold liquid chlorine and one ton containers hold sulfur dioxide. The chief executive said each container that leaves one of the company's 11 productions facilities is photographed and the photo is filed with its serial number. City workers sent containers back to the company's Milford, Virginia, plant because of valves they could not open. The deputy director of operations for the city's department of public works told the aldermen that plant workers referred to standards set by the Chlorine Institute when identifying unsafe containers. Plant workers also had problems sealing the connections with the containers, creating greater risk for leaks, according to a letter the city sent to the company on November 12. The chief executive maintains his company provided a product that met safety standards.
   Source: http://www.wtop.com/?nid=25&sid=1532777

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *December 2, Seacoastonline.com* – (New Hampshire) **Hunters violate nuclear security zone.** Three armed duck hunters in a boat got close enough to FPL Energy Seabrook Station on Tuesday morning for nuclear power plant security, local police, and the Coast Guard to respond. One of the hunters stepped out of the boat, according to information released by the Coast Guard. The incident happened around 9 a.m. on Tuesday, December 2. Seabrook Station has a security zone within 250 yards of the nuclear power plant, said a lieutenant of Marine Safety Detachment out of New Castle. There are signs in the marsh but no fencing, he said. As of Tuesday night, no charges had been brought against any of the men. If charges were brought, he said, they would come from the Coast Guard. "We're going to investigate and question the men whether they saw the signs," he said. "They never said whether they did." A Seabrook police sergeant said, "The duck hunters got close to the perimeter…There was no trespass, no charges. They were on the banking, in and out of the boat." The men were armed with shotguns, he said. "Our only response is, at no time was safety or the security of plant in jeopardy," said a Seabrook Station spokesman.
   Source: http://www.seacoastonline.com/articles/20081202-NEWS-81202038

6. *December 2, Reuters* – (South Carolina) **Progress SC Robinson 2 reactor exits outage.** Progress Energy Inc.'s Unit 2 at the Robinson power station in South Carolina

exited an outage and ramped up to 94 percent power by early Tuesday, the U.S. Nuclear Regulatory Commission said in a report. The unit shut November 17 due to high turbine vibration.
Source: http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSN02547696200812 02

7. *December 2, U.S. Nuclear Regulatory Commission* – (Florida) **Fitness for duty.** A non-licensed employee supervisor at the Turkey Point nuclear power plant in Florida had a confirmed positive for illegal drugs during a follow-up fitness-for-duty test. The employee's access to the plant has been denied. The licensee notified the U.S. Nuclear Regulatory Commission resident inspector.
Source: http://www.nrc.gov/reading-rm/doc-collections/event-status/event/2008/20081203en.html#en44691

[Return to top]

Defense Industrial Base Sector

8. *December 3, Coast Guard News* – (Alabama) **EADS North America to expand its Mobile, Alabama facility.** EADS North America will further expand the company's U.S. industrial presence with the construction of a new 27,000-sq. ft. aircraft maintenance delivery center at the Mobile, Alabama, facility of its EADS CASA North America business unit. This $5.6 million facility expansion, located at the Mobile Regional Airport, will provide a modern support, overhaul, and modification center for the growing number of EADS CASA multi-role transport aircraft operated by government and civilian customers in North, Central, and South America — including the U.S. Coast Guard. Groundbreaking for the new center is planned for early 2009, with the completion targeted by year end. EADS CASA's family of twin-engine transport aircraft are employed in a variety of missions by customers in North, Central, and South America, including passenger and cargo transport, paratroop training, and utility purposes. The U.S. Coast Guard will become one of the world's largest operators of EADS CASA products, acquiring an expected fleet of 36 HC-144A Ocean Sentry maritime surveillance aircraft. Six of these twin-engine, medium-range platforms already have been delivered to the Coast Guard, with operational test and evaluation now underway in preparation for the Ocean Sentry's service introduction.
Source: http://coastguardnews.com/eads-north-america-to-expand-its-mobile-alabama-facility/2008/12/03/

9. *December 1, Knoxville News Sentinel* – (National) **Y-12 security not on IG's hit list.** A new report by the Department of Energy's Inspector General criticized three sites (two National Nuclear Security Administration [NNSA] and one non-NNSA) where protective force officers were not trained to use their 40 mm grenade launchers under reduced visibility (night conditions). The IG report did not name the sites for security reasons. However, a federal spokesman at the Y-12 nuclear weapons plant said Y-12 was not in the wrong, saying "SPOs (security police officers) protecting Y-12 train under all conditions, including low-light situations." A spokeswoman for security

contractor Wackenhut Services said the Oak Ridge team is "fully compliant" for training regulations associated with the grenade launchers. Wackenhut Services provides protective services at all of the Oak Ridge sites under two contracts (one for Y-12, one for the other DOE sites). She said she could not discuss which weapons are deployed at which sites, but said the contractor was in full compliance on this training issue.
Source:
http://blogs.knoxnews.com/knx/munger/2008/12/y12_not_on_igs_hit_list_this_t.html

[Return to top]

Banking and Finance Sector

10. *December 3, KXII 12 Sherman* – (Texas) **Bank links over 400 identity theft cases to Gainesville restaurant.** Gainesville police say there have been over 30 cases of identity theft in just the past month, and one restaurant in Gainesville has put about 400 customers in danger of being victims of identity theft. One Gainesville bank official says Golden Chick has put 400 of its customers were in danger of identity theft between October and mid-November. First State Bank in Gainesville received a number of phone calls from their customers about transactions they never made. It turned out they were victims of fraud. First State Bank investigated all of their customers' accounts and found there were more people in danger than they expected. "We had a list of accounts that reported the fraud, so we pulled transactions back from an earlier point in time, and we noticed that a common denominator that all these customers went to Golden Chick," a senior vice president at First State Bank of Gainesville says.
Source: http://www.kxii.com/home/headlines/35421434.html

11. *December 3, Register* – (International) **Online payment site hijacked by notorious crime gang.** Online payment service CheckFree lost control of at least two of its domains on Tuesday in an attack that sent customers to servers run by a notorious crime gang believed to be based in Eastern Europe. A regular reader reported receiving a bogus secure sockets layer certificate when attempting to log in to his Mycheckfree.com account early Tuesday morning. On further examination, he discovered the site was mapping to 91.203.92.63. To confirm the redirection was an internet-wide problem, he checked the site using a server in another part of the U.S. and got the same result.
"I managed to get through to a commercial customer support tech, and reported the problem," the reader wrote in an email sent early Tuesday morning. "He was not aware of any problem." The account is consistent with results of passive DNS search queries. Security experts say the 91.203.92.63 IP address has long served as a conduit for online crime.
Source: http://www.theregister.co.uk/2008/12/03/checkfree_hijacked/

12. *December 3, KOMO 4 Seattle* – (Washington) **Beware of phishing scams by crooks posing as banks.** While banks work to clean up their money mess, con artists are working to clean out your account. They are focusing on customers of Washington

Mutual and JP Morgan Chase, but every bank customer is a potential target. It is a new wave of email "phishing" that claims to be from Chase bank. One email promises $50 for answering an online banking survey. Click to answer and one gets what looks like an official survey from Chase bank asking for account information — it is a fake. Another email claims to be an account verification alert. Unlike previous imposter scams which claim there has been a security breach or technical problem, this latest version goes to extra lengths to tie in the economy, with an elaborate explanation about the financial crisis, and a threat, that unverified accounts will be shut down in three business days. By using the Chase name, scammers are reaching potentially millions of costumers of JP Morgan Chase, and recently acquired Washington Mutual. And, in what may be a first, the scammers are using the name of an actual Chase executive. The email is signed by the chief operations officer. In a statement, a bank spokesperson said, "It is definitely not a legitimate email, as you already know."
Source: http://www.komonews.com/news/consumer/35442584.html

13. *December 3, CNNMoney.com* – (National) **AIG, Fed stemming insurer's liquidity crisis.** Troubled insurer American International Group moved another step closer to stabilizing its finances on Tuesday. The company announced that a financing entity — funded by the Federal Reserve Bank of New York and AIG — has purchased $46.1 billion in complex debt securities insured by AIG. As part of the deal, the insurance-type contracts, called credit default swaps, were terminated. The insurer also has agreements to purchase another $7.4 billion of these debt securities, called collateralized debt obligations or CDOs. The move stanches some of the bleeding at the insurer, which was on the verge of bankruptcy in September because of these CDOs. As the debt securities' value declined, AIG was forced to post more collateral to prove to swaps holders it could pay them if the debt securities defaulted.
Source: http://money.cnn.com/2008/12/02/news/companies/AIG/index.htm

14. *December 3, Bank Technology News* – (National) **M&A surge jeopardizes sensitive data.** The recent wave of bank mergers is making protecting data all the more difficult. It is hard to imagine a more likely time for security holes to open up than when two banks — rife with legacy systems, custom patches, and unique protocols — try to mesh it all together. To make matters worse, mergers usually result in layoffs, and disgruntled, soon-to-be ex-employees will be tempted to take advantage of any security lapse. The chief scientist at RedSeal Systems, a company that develops proactive security risk management software, refers to these as "toxic networks." If an acquired company has a different approach to security "you could be taking on a problem every bit as bad as toxic assets...If you attach to a network that is unacceptably weak, now you are weak." Each network needs to be reconstructed so IT personnel can have a complete view of all the networks to locate the best pathways to connect the networks, while securing assets and regulating who has access to which assets. As risky and intensive as linking networks is, the chief scientist and others note that IT personnel are under incredible pressure to "parachute in" and act fast. They must assess the risk, do it quickly, often examining an unfamiliar structure.
Source: http://www.americanbanker.com/btn_article.html?id=20081202LQTUGON6

15. *December 3, Oxford Press* – (Ohio) **FBI involved in Mason firm's ID theft case.** The FBI has become involved in an identity theft case involving a Mason, Ohio, eye wear retailer. The Federal Bureau of Investigation became involved Tuesday in the investigation of Luxottica's computer servers after a hacker tapped into them, said a Hamilton Township lieutenant, who heads the Warren County Cyber Crimes Task Force. The hacker grabbed personal information from about 59,000 former employees, he said. He said he was called in by Luxottica's technology staff in September, after they discovered the breach. The server contained information — such as Social Security numbers and addresses — for 59,419 employees of the Things Remembered retail chain, a subsidiary of Luxottica, whose retail headquarters is in Mason, he said. Investigators traced the breach to an IP address owned by a resident of the Glendale, Arizona, area. However, he was careful to note that person might not have been the one on the keyboard.
Source:
http://www.oxfordpress.com/hp/content/oh/story/news/local/2008/12/03/pjm120408luxottica.html

16. *December 2, Computerworld* – (International) **Feds nab more members of alleged identity theft gang.** Federal authorities say they have taken another step toward busting a multinational identity theft ring that is alleged to have used stolen personal data to withdraw millions of dollars from home equity line-of-credit accounts at dozens of financial institutions in the U.S., including some of the country's largest banks. Four individuals were arrested last week in connection with the alleged scheme, which has resulted in more than $2.5 million being stolen from the affected financial institutions, according to law enforcement officials. Another $4 million worth of attempted withdrawals by the gang were unsuccessful, the U.S. attorney's office in New Jersey said in announcing the arrests last Wednesday. Court documents filed in connection with the case described an operation that appears to have been highly sophisticated and global in nature. The identity theft gang operates in the United States as well as the United Kingdom, Canada, China, Japan, Vietnam, South Korea, and several other countries, the court documents said. Four other men already were charged with participating in the scheme after being arrested between August and October.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9122121&intsrc=hm_list

17. *December 2, ARS Technica* – (National) **Odd microtransactions may point to credit card breach.** A wave of unauthorized microtransactions is currently sweeping the accounts of a number of U.S. credit card holders, though the size and scope of the fraud scheme have not yet been determined. Beginning on or around November 20, consumers apparently began to notice small charges—typically for 19-29 cents—appearing on their bank statements or online account information. These small withdrawals or deposits are typically test fees, sent to verify account authenticity. Paypal, for example, makes two small deposits in a user's bank account in order to verify its authenticity. While legitimate companies will reverse the fee (or occasionally let you keep the extra quarter), thieves use the transactions to verify that a credit card

number is good. If the deposits complete successfully, the hacker knows he has got a live card (or a live card number). The next step is usually to burn through the account's balance as quickly as possible before anyone notices what is happening. Beginning on or about November 20, various card holders began complaining online about unauthorized microtransactions that were suddenly showing up on their accounts. The charges fit the model described above, and were labeled as coming from Adele Services. Adele Services appears to be a dummy corporation; the 1-800 number listed as the customer contact point is disconnected and there is no official website. The company may not officially exist, but that has not stopped it from continuing to test accounts. It is impossible to state how many card holders have been pinged in this manner, but the number of online reports is growing steadily. Theories on which company's security was breached abound, although PayPal has been collectively ruled out, given the number of non-PayPal users affected. Amazon seems to be a current favorite, based on the fact that a number of the irate forum posters recently shopped there.
Source: http://arstechnica.com/news.ars/post/20081202-odd-microtransactions-may-point-to-credit-card-breach.html

[Return to top]

Transportation Sector

18. *December 3, Associated Press* – (Missouri) **Airliner lands safely with shattered windshield.** A regional airliner with a cracked windshield was diverted to Kansas City's airport and landed safely Tuesday. No injuries were reported. United Express Flight 5335 was carrying 66 passengers and four crew members on a flight from St. Louis to Denver. The windshield was cracked but still in place when the Bombardier CRJ-700 Canadair jetliner reached a gate, a spokesman for Kansas City International Airport. The spokesman said the airline launched an investigation to find how the windshield broke. He could not say when in the flight the cracks occurred, whether an object struck the windshield, or if any shards of glass came loose in the cockpit.
Source: http://www.msnbc.msn.com/id/28015147/

19. *December 2, Federal Times* – (National) **Mumbai attack shows need to secure small boats, DHS leaders say.** The top leaders of the Homeland Security Department and Coast Guard say the deadly assault last week in Mumbai, India, emphasizes the need to counter the threat of attacks involving the use of small boats. The assault "underscores the importance of what we're doing at our ports in terms of security," the Homeland Security Secretary said. The terrorists who attacked hotels and other establishments in Mumbai are thought to have arrived in the city by boat. The U.S. Coast Guard Commandant said he is pressing the international community, as well as boating communities in the United States, on the need to have small boats — those under 300 gross tons — carry identifying transponders so security forces can better monitor those that may be potential threats.
Source: http://www.federaltimes.com/index.php?S=3845701

20. *December 2, WFLX 29 Palm Beach* – (Florida) **Security tightens: 100 miles of**

Florida Railway. The Palm Beach County Sherriff's Office is one of two dozen federal, state, and local law enforcement agencies taking part in "Operation Transit Shield" Tuesday. The initiative is an anti-terror effort involving hundreds of law enforcement agents patrolling nearly 100 miles of railway in Palm Beach, Broward, and Miami-Dade counties. A spokesman added that it's always important that the public remain on alert — and vigilant, despite the fact that there has never been an attack on south Florida's railway system. The push kicked off at 6:30 a.m. Tuesday and stretched through the morning commute at local train stations and local railways. Not all of the stepped-up security will be visible to the public, officials said. "Operation Transit Shield" is coordinated by members of the Southeast Regional Domestic Security Task Force which includes law enforcement from the Palm Beaches all the way down to Miami.
Source: http://www.wflxfox29.com/Global/story.asp?S=9443214&nav=menu98_3

21. *December 2, Houston Chronicle* – (Texas) **Red-Light cameras cut wrecks 30%.** Red-light cameras have sprouted quickly across Texas in recent years, sparking heated debates about whether they reduce crashes or simply bring easy revenue for the cities that install them. A statewide study by institute researchers shows that monitored intersections had an overall 30 percent decrease in collisions. The state-mandated report, released Tuesday by the Texas Department of Transportation, examined data from 56 intersections across the state, including many in Houston, from July 1, 2007, to June 31. The data and analysis are limited because some cities' cameras went online during the study period and their post-installation data were not complete. But the report states that the cameras could be changing driver behavior.
Source: http://www.chron.com/disp/story.mpl/front/6144100.html

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

22. *December 3, USAgNet* – (Indiana) **Bovine TB case traced to Indiana farm.** Staff of the Indiana State Board of Animal Health (BOAH) is investigating a case of bovine tuberculosis (commonly called "TB," or more formally known as Mycobacterium bovis) in a beef cattle herd in Southeastern Indiana. The TB-positive cow was identified through routine testing at a meat processing facility in Pennsylvania. BOAH veterinarians are in the very early stages of conducting a thorough investigation of the animal's movements within the state. Few details are currently known about the herd. Indiana has held a bovine tuberculosis-free status since 1984 with the U.S. Department of Agriculture. Under federal guidelines, that status remains. The last time a Hoosier herd tested positive for the disease was in the 1970s.
Source: http://www.usagnet.com/story-national.php?Id=2811&yr=2008

23. *December 2, Cattle Network* – (International) **AMI: U.S. & Mexican facilities approved for meat export.** The United States and Mexico have reached an agreement on approving a significant number of meat processing and storage facilities for export. The U.S. Food Safety Inspection Service (FSIS) and Mexico's food safety agency, SAGARPA, have been involved in ongoing discussions over the past 18 months to resolve this issue. In the United States, discussions have involved 109 U.S. meat industry facilities, of which 52 have now been approved for export and another 57 facilities that are expected to be approved in the coming week. This action comes on the heels of approval by SAGARPA of administrative changes at 32 U.S. facilities. In Mexico, 13 facilities have been approved, although four of those approvals are pending corrective action. This will bring the total of Mexican meat facilities approved for exporting to the United States to more than 30.
Source: http://www.cattlenetwork.com/Content.asp?ContentID=273022

24. *December 2, Reuters* – (Kansas) **Fight over adding hormones, labeling milk rages on.** Anti-biotech forces turned out in Kansas on Tuesday to argue against a state plan that would limit how dairy products free from artificial hormones can be labeled. The Kansas Department of Agriculture held its final hearing on the matter Tuesday morning, considering a regulation that would ban dairy product labels from stating the product as "rBST free." The law would take effect in January 2010. In addition to banning "rBST-free" claims, the rule would require that labels declaring products to have been derived from cows not supplemented with the growth hormone to carry companion disclaimers saying "the FDA has determined that no significant difference has been shown between milk derived from rBST-supplemented and non-rBST-supplemented cows." Biotech backers have been fighting back, arguing that artificial hormones help cows produce more milk, do not create health problems for the animals or humans and argue that labels making a distinction needlessly confuse consumers when there is no discernible difference in products derived from cows that receive the hormones and those that do not. A coalition of more than 90 groups representing dairy farmers, consumers groups, farm, agricultural and environmental organizations, food processors and retailers submitted a letter to the Kansas governor to oppose the new rules.
Source: http://www.cnbc.com/id/28019760

25. *December 1, Produce News* – (International) **Romaine lettuce 'prime suspect' in E. coli outbreak in Ontario.** Canadian and U.S. officials are investigating an E. coli outbreak that has sickened 30 people, nine of whom were hospitalized, in southeastern Ontario. The acting national manager of the Canadian Food Inspection Agency's fresh fruit and vegetable program said that though the investigation was not completed, "through epidemiological studies, Romaine [lettuce] is basically the prime suspect." The investigation has centered on Romaine grown in California, and a spokesperson for the California Department of Public Health (CDPH), told the Produce News November 24 that "in cooperation with the U.S. Food & Drug Administration, the CDPH is following up on information received from Canadian health officials regarding a foodborne outbreak of E. coli 0157:H7 illness in Canada potentially linked to Romaine

lettuce. CDPH is currently conducting a farm investigation based on the information supplied by Canadian authorities." The Canadian Food Inspection Agency's fresh fruit and vegetable program said that the inspection agency was working with the FDA, and the Public Health Agency of Canada was working with the U.S. Centers for Disease Control and Prevention to determine the source of the problems. At this stage of the investigation, he said, the inspection agency was responsible for working on traceability, and as soon as studies led to Romaine, the agency began taking samples of product grown in Salinas, California, at wholesalers and foodservice distributors in the Toronto area. While the investigation is still ongoing, a spokesperson for the Ontario Ministry of Health and Long Term Care said that "no source has been confirmed.
Source: http://www.theproducenews.com/StoryNews.cfm?ID=8338

[Return to top]

Water Sector

Nothing to report

[Return to top]

Public Health and Healthcare Sector

26. *December 2, New York Times* – (National) **Expert panel seeks changes in training of medical residents.** A national panel of medical experts proposed significant and costly changes for training new doctors in the nation's hospitals, recommending mandatory sleep breaks and more structured shift changes to reduce the risk of fatigue-related errors. The experts' report, issued by the Institute of Medicine on Tuesday, focused on the grueling training of medical residents, the recent medical school graduates who care for patients under the supervision of a fully licensed physician. The medical residency, which aims to educate doctors by immersing them in a particular specialty and all aspects of patient care, is characterized by heavy workloads, 80-hour workweeks, and sleep deprivation. The worry is that the huge workload imposed on residents poses a risk to patient safety. The long hours of often unsupervised residents were found to have contributed to the 1984 death of an 18-year-old in New York City, a finding that eventually led to a series of changes, including limiting residents to an 80-hour workweek and 30-hour shifts. But the expert panel said those reforms were not enough. Caps on work hours are often not enforced, and many residents still do not get enough sleep, putting doctors and patients at risk for fatigue-related mistakes. While the new recommendations do not reduce overall working hours for residents, the report says no resident should work longer than a 16-hour shift, which should be followed by a mandatory five-hour nap period.
Source: http://www.nytimes.com/2008/12/03/health/03doctors.html?ref=us

27. *December 2, Associated Press* – (National) **Anthrax case sparks training at Army labs.** Workers who handle dangerous pathogens at Army biological research laboratories will get additional security training in the wake of the Federal Bureau of Investigation's finding that an Army scientist was behind the 2001 anthrax attacks,

military officials said Tuesday. A weeklong refresher course began Monday at the flagship biodefense lab at Fort Detrick in Frederick, Maryland, where a microbiologist allegedly obtained and refined the anthrax used in the deadly mailings, the laboratory's spokeswoman said, adding that additional training in security, accounting, and reporting rules will be given at five other Army labs over the next few months. She said Army leaders are not calling for changes in pathogen handling but are reiterating procedures for inventory and documentation. A special assistant to the Army Secretary said the training was recommended as a first step by a task force reviewing biolab security practices in response to the anthrax case. The laboratory spokeswoman said Fort Detrick's lab, the U.S. Army Medical Research Institute of Infectious Diseases has strengthened its security procedures since the anthrax attacks.
Source: http://www.msnbc.msn.com/id/28018252/

[Return to top]

Government Facilities Sector

28. *December 3, Destinlog.com* – (Florida) **Hurlburt discovers bomb after anonymous tip.** The Okaloosa County Sheriff's Office and Hurlburt Office of Special Investigation discovered an explosive device in the back of a truck that had base access after receiving an anonymous tip Tuesday morning. At about 6 a.m., deputies received an untraceable call and alerted Hurlburt Security personnel of the potential danger. The male voice had warned that a man working at Hurlburt Field had explosives on his truck. Hurlburt Field security levels were raised at 10 a.m. when morning searches for the truck came up empty. The caller's partial description eventually led investigators to a man with access to the base through his employers who had a construction contract. By 10:40 a.m., deputies spotted the truck in the Consul Apartments parking lot on Monahan Drive. The owner of the truck denied any knowledge of an item investigators found in the back of his vehicle. A military working dog searched the truck but did not detect the explosives. As a precaution, deputies evacuated the buildings, established a 1,000-foot-perimeter with road blocks on Monahan Drive, and told residents across the street to stay inside. The evacuation remained in effect until the bomb was diffused. The incident is under investigation by the U.S. Bureau of Alcohol, Tobacco and Firearms.
Source:
http://www.thedestinlog.com/news/hurlburt_7205___article.html/truck_link.html

29. *December 2, WFTV 9 Orlando* – (Florida) **Agency accidentally posts 250,000 SS numbers online.** Social security numbers for 250,000 people were posted online by mistake, and a state agency is facing serious questions about why it was so careless with the information. The Agency for Workforce Innovation accidentally posted the sensitive information for people looking for work. All those numbers were left online for at least 19 days. Potential victims do not even know it yet. When thousands of Floridians went to a career center, their personal information was forwarded to the state. Then, by mistake, that information ended up on a state website visible to anyone with Internet access. Local jobseekers' identities have been compromised. Names, social security numbers, and employment information of more than 250,000 people

who sought state help was accidently posted online. The Washington D.C. based Liberty Coalition spotted the error. “This is obviously a case of gross negligence,” said a spokesman for the Liberty Coalition. The Florida Agency for Workforce Innovation made the mistake in October when setting up a computer server. Somehow information that should have been kept private became public, available by an online search. It has since been taken down. The security breach affects people who went to a career service center between 2002 and 2007; even the identities of some their children were posted online. The Florida Agency for Workforce Innovation says it will send out a letter to all the people affected by the breach.
Source: http://www.wftv.com/news/18190154/detail.html#-

30. *December 2, Ocala Star-Banner* – (Florida) **Bomb squad explodes package at Marion County Jail.** The Marion County, Florida, Jail was on lockdown Tuesday night due to a suspicious package that was thrown against the west side of jail by an unidentified man. Deputies said that around 7:30 p.m. a small blue car pulled up to the gate to the jail complex and a man said that he was going to visit an inmate. He was allowed to drive toward the jail. Then officials noticed that he threw a rectangular shaped package on the west side of the fence. The man sped off, and deputies immediately called for Ocala Fire Rescue and the Sheriff’s Office Bomb Squad. The Bomb Squad robot was deployed to the gate to the jail complex. It exploded the package in place at 9:05 p.m. Sheriff’s officials said the box contained a small battery, wires, and clothing.
Source: http://www.ocala.com/article/20081202/ARTICLES/812020276/-1/SPORTS02?Title=Bomb_Squad_explodes_package_at_Marion_County_Jail

31. *December 2, WPSD 6 Paducah* – (Kentucky) **McCracken County Jail lobby evacuated because of suspicious package.** The McCracken County Jail’s lobby was evacuated Tuesday because of some suspicious packages dropped off. Around 11 o’clock, a man dropped off packages wrapped with Christmas paper and put together with purple duct tape. The packages were addressed to two area judges. The lobby was evacuated as a precaution. The packages were suspicious enough to lock down the jail and bring in the Paducah Bomb Squad. It turns out they did not contain explosives or anything dangerous, but when the bomb squad arrived and took x-rays of the packages, they were not able to determine what was inside. Uncertain of the packages content, they decided to remote detonate. They used a water cannon to blow apart the packages inside the lobby.
Source: http://www.wpsdlocal6.com/news/local/story.aspx?content_id=db9aa0ca-18fb-47f0-89f5-662ddb368ea2

[Return to top]

Emergency Services Sector

32. *December 2, WTOP 103.5 District of Columbia* – (District of Columbia) **Maryland medevac transports drop since fatal crash.** The number of Maryland medevac transports has dropped significantly since a fatal crash in September, and lawmakers are now wondering if they should proceed with plans to replace the entire aging

helicopter fleet. There have been 396 requests for medevac flights since the crash in District Heights that killed four of the five people aboard. About 57 percent of those requests resulted in transports. If that trend continues, there would be about 1,679 transports a year — a major drop from the 4,100 transports last year. The state's fleet currently includes 11 helicopters.
Source: http://www.wtopnews.com/?nid=25&sid=1533991

33. *December 2, WFOR 4 Miami* – (National) **First responders practice for bio-terrorism attack.** The Emergency Medical Learning and Resource Center (EMLRC), a non-profit organization based in Orlando, is in Hollywood, Florida, this week training Hollywood Fire Rescue teams in dealing with a biological attack. The training uses an interactive mannequin called "Tom" as a patient simulator. Paramedics and EMTs ask Tom questions about how he's feeling, and, based on his responses, diagnose him. They can also help him breathe, give him CPR, take his pulse and can even give him medication. The training coincides with a report issued Tuesday by a bi-partisan commission appointed after the 9/11 attacks, which said the United States could face a biological or nuclear attack within the next five years.
Source: http://cbs4.com/local/tom.terrorist.attack.2.878519.html

34. *December 2, TMCnet* – (Texas) **Rescue robots tested for search and recovery missions.** A rescue robot exercise was conducted recently in Disaster City, Texas, by the National Institute of Standards and Technology (NIST) in an effort to develop performance standards for robots for use in urban search and rescue missions. During the testing program, close to three dozen robots were evaluated by developers and first responders. Urban search and rescue robots help first responders by carrying out tasks like entering partially collapsed structures to find survivors or to identify poisonous chemicals. NIST is creating robot standards for testing along with industry and government partners. The site of the event, Disaster City, Texas, is a test facility operated by the Texas Engineering Extension Service (TEEX). It features an airstrip, lakes, train wrecks, and rubble piles that can be arranged for many types of challenging tests. Developers tested battery capacity by having robots perform figure eights on a rising and falling terrain and mobility tests in which robots ran through increasingly challenging exercises beginning with climbing steps and escalating to climbing ramps and then making it up steps with unequal gaps.
Source: http://robotics.tmcnet.com/topics/robotics/articles/46507-rescue-robots-tested-search-recovery-missions.htm

[Return to top]

Information Technology

35. *December 3, Heise Security* – (International) **Adobe admits Acrobat 9 passwords can be guessed more quickly.** Adobe recently replied to the online discussion of Acrobat's vulnerability to brute-force attacks. Adobe claims that the specification for the 256-bit AES encryption in Acrobat 9 provides greater performance than the 128-bit implementation in previous versions. It is this improved performance that allows Acrobat 9 to open protected documents much more quickly. Adobe has admitted that

brute-force attacks and dictionary-based password cracks benefit from the program's extra speed, because "fewer processor cycles are required" to test each password guess than with AES 128-encrypted documents. Adobe does not say how much faster attacks can be carried out, but Elcomsoft, a manufacturer of password-recovery tools, claims that passwords can now be cracked 100 times faster. To help mitigate dictionary attacks, Adobe advises customers to use long passwords or pass-phrases. Version 9 supports Unicode pass-phrases up to 127 characters in length. For even greater security, Adobe recommends using encryption based on the Public Key Infrastructure, although this requires the use of Adobe LiveCycle Rights Management.
Source: http://www.heise-online.co.uk/news/Adobe-admits-Acrobat-9-passwords-can-be-guessed-more-quickly--/112138

36. *December 3, Blackberry Cool* – (International) **BlackBerry Desktop Software contains critical security flaw.** RIM has posted a knowledge base article describing a critical security flaw within the BlackBerry Desktop Software. The flaw has been confirmed by Secunia, a leading vulnerability intelligence provider. Here's the problem as described by RIM: "The BlackBerry Desktop Manager includes the Roxio Media Manager for managing media synchronization between the BlackBerry smartphone and the Microsoft Windows computer. The Roxio Media Manager includes a Microsoft ActiveX control used for retrieving and installing application updates. A buffer overflow exists in the DWUpdateService ActiveX control that could potentially be exploited when a user visits a malicious web page that invokes this control."
Source: http://www.blackberrycool.com/2008/12/blackberry-desktop-software-contains-critical-security-flaw/

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

37. *December 2, Space.com* – (International) **Russians track wayward U.S. spy satellite.** The U.S. Air Force apparently has a malfunctioning Defense Support Program satellite on its hands. DSP-23 is one piece of a constellation of such Earth-staring satellites designed to detect missile launchings and nuclear detonations, and gather other technical intelligence. DSP-23 seems to be drifting out of its high-altitude slot — and might prove troublesome to other high-value satellites in that populated area. One person who has flagged the problem to a U.S. satellite tracking expert is a Russian space analyst — a project partner of the International Scientific Optical Network (ISON). He said ISON is monitoring the entire ring of objects in geostationary Earth orbit (GEO). The network tracks all operational satellites, as well as space debris, spent rocket bodies, dead spacecraft, operational fragments, and objects originating from

satellite fragmentations that have appeared in geostationary orbit. “We have continuously tracked an object we have identified as DSP F23 since January 10, 2008,” he said. The spacecraft has strayed from its spot in space — moving along in geostationary orbit as a passive object. It is not clear from optical data alone just what the operational status of the satellite truly is at present, he added. Asked about the possibility of DSP-23 smacking into others satellites in GEO, he said that “it exists.” Sauntering willy-nilly through space, the classified satellite could have close encounters with many operational satellites, he said.
Source: http://www.msnbc.msn.com/id/28023768/

[Return to top]

Commercial Facilities Sector

38. *December 3, Associated Press* – (National) **India siege raises security concerns at U.S. hotels.** The response by the New York Police Department to quickly shore up security with a show of force outside the Waldorf Astoria, New York Palace, and other marquee hotels after news of the Mumbai attacks, though strictly precautionary, demonstrated that the deadly attack in India had far-reaching implications for police and private security officials in New York and other U.S. cities. The 535-room Drake Hotel in Chicago reviewed its security measures in the wake of the attacks and “realigned” some security staff, a marketing manager at the Drake said. In Los Angeles, police have been studying the Mumbai attacks and are considering sending investigators there to learn more. Police in New York and Los Angeles have programs to share intelligence and security tips with large businesses, including hotels, through Web sites, closed-door briefings, and seminars. The NYPD also has beefed up patrols outside major hotels since the attacks in India. Unlike fortified hotels in international trouble spots, the U.S. hotels have not resorted to heavily armed guards, checkpoints or other drastic measures to deter terror. Besides what is visible — plainclothes security agents and surveillance cameras — major chains are reluctant to give specifics about their security. It is unlikely that any hotel, no matter how exemplary its security, could fend off a concerted, Mumbai-style attack on its own, said the co-owner of Elite Protection, an Illinois-based security firm that counts several large Chicago hotels as clients.
Source: http://www.iht.com/articles/ap/2008/12/02/america/India-Shootings-Hotel-Security.php

39. *December 2, WFTV 9 Orlando* – (Florida) **Residents evacuated as crews search subdivision for bombs.** Crews are again searching for bombs near Odyssey Middle School and dozens of residents could not go home all day. The new search for old bombs forced a dozen families out of their homes early Tuesday morning. The Army Corps of Engineers searched behind their houses in the Lee Vista Square subdivision for more explosives. The Corps revealed late Tuesday afternoon that it found one 75-millimeter practice projectile and they will be searching again on Wednesday. A bullet, about 3 inches around, found two weeks ago near a retention pond sparked the search and evacuation. It was reportedly harmless. Eyewitness News has been following the story since July 2007. Surveyors have found more than 220 bombs and 14 tons of

munitions on the old Pine Castle Jeep Military Range. The Army Corps of Engineers plans to continue searching in the same area Wednesday. Homeowners will have to be out by 8:00 a.m. They have made arrangements for people to stay in a common area at the Springhill Suites on Hazeltine National Drive near the airport. They said the entire process, so far, including the investigation, has cost them more than $12 million.
Source: http://www.wftv.com/news/18186922/detail.html#-

40. *December 2, Associated Press* – (Ohio) **Police: 2 homemade bombs dismantled in Ohio town.** A homemade bomb was found Tuesday at a gas station a block away from a school, and authorities arresting a suspect found a second bomb on the man's body, police said. The 18 year old man arrested had been convicted in 2006 of taking explosives to a different school where he said he had been the subject of ridicule. Someone left a backpack near pumps at a gas station in St. Marys, and a customer took it to employees, the manager said. After about 45 minutes, employees looked inside, found a bomb, and called police, the manager said. The explosive device was made of fluid-filled bottles and a detonator, the police chief said. Nearby residents were evacuated. Police later arrested the man at his apartment, where they dismantled a second, smaller homemade bomb discovered under his shirt. Both bombs were dismantled, and no one was injured, police said. Authorities would not say whether the bombs were part of a larger plot or whether the school was an intended target. Police did not know how much damage the device left at the Marathon gas station could have caused or whether it was close to being detonated.
Source: http://www.mercurynews.com/nationworld/ci_11122215

41. *December 2, San Diego Union Tribune* – (California) **Chemical explosion in Santee snarls traffic.** Traffic along Santee's busiest street, Mission Gorge Road, came to a standstill following a chemical explosion behind a building Tuesday afternoon. Mission Gorge was closed in both directions between Cottonwood and Magnolia avenues following the 12:35 p.m. incident. The Santee Deputy Fire Chief said a mixture of swimming pool chemicals including liquid and powder chlorine caused an explosion behind a building, sending the chemicals into the air. About a dozen businesses had to be evacuated in the area, and residents in a nearby mobile home park were asked to stay indoors. Four sheriff's deputies and one firefighter were taken to a hospital after they experienced respiratory irritation and a burning sensation in their eyes. A four-block stretch of Mission Gorge Road was expected to be closed well into rush hour while hazardous materials crews cleaned up the mess.
Source: http://weblog.signonsandiego.com/news/breaking/2008/12/chemical_explosion_in_santee_s.html

[Return to top]

National Monuments & Icons Sector

42. *December 2, U.S. Forest Service* – (California) **News Release: Marijuana grower sentenced to 10 years.** On Monday, December 1, 2008, in the Eastern District Court of California, a father and son were sentenced in federal court for the manufacturing of

marijuana on the Six Rivers National Forest, receiving 57 and 120 months' prison time, respectively. The men were arrested on July 4, 2007 by law enforcement officers from the U.S. Forest Service, Trinity County Sheriff's Department, and California Department of Fish and Game. Officers entered the marijuana garden located near Zenia, California, and found the two suspects armed with rifles working in the marijuana garden. The men told investigators that they had been living on the National Forest since May 2007, growing their marijuana. The marijuana garden contained a camp and kitchen area that was stocked with large amounts of food and supplies. Also found near the garden were large amounts of garbage discarded in the forest.
Source: http://www.fs.fed.us/r5/sixrivers/news/2008/12/02/

[Return to top]

Dams Sector

43. *December 3, Solon Herald Sun* – (Ohio) **Solon: Repairs to Briar Hill Lake dam have yet to begin.** Repairs to the dam on Briar Hill Lake will not get done by the end of 2008, as required earlier this year by the Ohio Department of Natural Resources (ODNR). In fact, construction has not even started. The city and the Briar Lake Association — the homeowners association for the Briar Hill subdivision — are still ironing out agreements as legal costs mount. However, the ODNR has extended its deadline indefinitely because progress is being made, according to an ODNR spokesperson.
Source:
http://blog.cleveland.com/solonheraldsun/2008/12/solon_repairs_to_briar_hill_la.html

44. *December 3, Daily Citizen* – (Wisconsin) **Repairs and improvements progressing for Hustisford Dam.** The Hustisford Dam advisory committee reports progress with making various repairs and addressing improvements to deal with dam operations, maintenance, and emergency action plans. The advisory committee was established by the Hustisford Village Board to assist the village in meeting requirements set forth in the dam inspection report of the Wisconsin Department of Natural Resources (DNR). "The advisory committee held its first meeting in October," said the village trustee and committee chair. "We reviewed and discussed the DNR inspection report in detail and assigned responsibilities for each action item. We are making good progress and will have completed several of the required embankment repairs by the end of the year. Written plans for dam inspection, operations and maintenance and for emergency action will also be ready for review and approval by the DNR by year end. New elevation benchmarks have already been established." The committee is also discussing with engineering consultants the scope and details for a dam failure analysis. The analysis is required by the state and technical work must be performed by a registered engineer. The DNR inspection report also noted several cracks in the dam structure that will require concrete repairs. Both the concrete repairs and dam failure analysis are major work projects that will be conducted over the next two years.
Source: http://www.wiscnews.com/bdc/news/316777

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.
To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer